IN THE CLAIMS

Claims 1 - 6. (Withdrawn)

7. (Previously Presented) A method of securely receiving content data on a user's system from a web broadcast infrastructure with a plurality of channels, the method comprising the steps of:

receiving encrypted content data from a broadcast channel, wherein the encrypted content data is encrypted with a first encrypting key having a corresponding first decrypting key;

executing an emulator to enable a single player application of the encrypted content data to receive content data over the broadcast channel as if the single player application is receiving the encrypted content data from a telecommunication infrastructure, thereby enabling the single player application to perform the following steps regardless from where the encrypted content has been received:

transferring to a trusted third party an encrypted first decrypting key, which has been encrypted with a second encrypting key of the trusted third party;

receiving the encrypted first decrypting key, which has been decrypted by the trusted third party and re-encrypted with a user's system key; and

decrypting, in a tamper resistant environment of the single player application, the encrypted first decrypting key with the user's system key.

8. (Previously Presented) The method as defined in claim 7, further comprising receiving the encrypted first decrypting key over a computer readable medium which is different than the web broadcast channel.

9. (Previously Presented) The method as defined in claim 7, wherein the step of receiving includes storing on the user's system the encrypted content data for later decrypting by the player application.

10. (Previously Presented) The method as defined in claim 9, wherein the step of receiving the encrypted content data further comprises the sub-steps of:

determining a schedule for next broadcast of the encrypted content data selected;

setting a trigger to trigger the user's system to receive the next broadcast of the encrypted content data selected.

11. (Previously Presented) The method as defined in claim 10, further comprising:

receiving promotional metadata related to the encrypted content data over the broadcast channel;

selecting by a user, encrypted content data to be received related to the promotional offering metadata;

wherein the step of receiving encrypted content data includes receiving encrypted content data from a second broadcast channel-selected from the promotional metadata on the second broadcast channel and a time provided by the trigger.

12. (Previously Presented) The method as defined in claim 11, wherein the step of receiving encrypted content data from a second channel includes receiving data in a format compatible with DirecPC™.

13. (Previously Presented) The method as defined claim 11, wherein the step of receiving data from a second channel includes the sub-step of:

authorizing over a back channel that the user's system is authorized to receive the encrypted content data selected; and wherein the step of receiving the encrypted first decrypting key includes receiving the encrypted first decrypting key only if the user's system is authorized by the trusted third party to receive the encrypted content data selected.

14. (Currently Amended) The method as defined claim 11, wherein the step of receiving encrypted content data from a second channel further includes the sub-step of:

presenting to the user, the next time the user starts the user's system, a status if [[the]] current encrypted content data selected from the promotional metadata has been received on the user's system.

15. (Previously Presented) The method as defined in claim 7, wherein the step of receiving the encrypted content data, includes receiving the encrypted content data along with a network address of the trusted third party.

16. (Previously Presented) The method as defined in claim 7 further comprising receiving the encrypted first decrypting key over a broadcast stream.

17. (Previously Presented) The method defined in claim 7, wherein the tamper resistant environment forms reencrypted content data by reencrypting the content data with a locally generated player application encrypting key, wherein the locally generated player application key requires less processing utilization than the first decrypting key to provide real-time decryption of the content data.

18. (Previously Presented) The method defined in claim 15, wherein the first decrypting key has a timeout provision for decrypting the content data.

Claims 19 - 20. (Withdrawn)

21. (Previously Presented) A user's system for securely receiving data from a web broadcast infrastructure with a plurality of channels, comprising:

a receiver for receiving promotional metadata from a broadcast channel, the promotional metadata related to data available for reception;

a controller for controlling the receiver to receive encrypted content data from the broadcast channel, the encrypted content data selected from the promotional metadata, and wherein the encrypted content data has been previously encrypted using a first encrypting key having a corresponding first decrypting key, wherein the first decrypting key has been encrypted with a second encrypting key of a trusted third party;

a single player application for rendering the encrypted content data;

an emulator to enable the single player application of the encrypted content data to receive content data over the broadcast channel as if the single player application is receiving the encrypted content data from a telecommunication infrastructure, thereby enabling the single player application to perform the following steps regardless from where the encrypted content has been received:

transferring to the trusted third party the encrypted first decrypting key, which has been encrypted with the second encrypting key;

receiving the encrypted first decrypting key, which has been decrypted by the trusted third party and re-encrypted with a user's system key; and

decrypting, in a tamper resistant environment of the single player application, the encrypted first decrypting key with the user's system key.

decrypting, on the user's system in a tamper resistant environment, the encrypted first decrypting key with the user's system key;

wherein the tamper resistant environment forms reencrypted content data by reencrypting the content data with a locally generated player application encrypting key, wherein the locally generated player application key requires less processing utilization than the first decrypting key to provide real-time decryption of the content data.

22. (Currently Amended) The user's system as defined in claim 21, wherein the [[the]] encrypted content data, includes a network address of the trusted third party.

23. (Previously Presented) The user's system as defined in claim 21, wherein the controller further comprises:

a schedule derived from the promotional metadata wherein the schedule is used to control the receiver to receive encrypted content data from the broadcast channel.

24. (Previously Presented) The user's system as defined in claim 21, wherein the receiver is adapted to receive encrypted content data broadcasted in a format compatible with DirecPC™.

Claim 25. (Withdrawn)